AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of the Northern Mariana Islands

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
A Samsung Galaxy A04S cellphone that was found subsequent to a search incident to the arrest of Yan Juan Hu TAITANO

Case No. MC24 00019

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

A Samsung Galaxy A04S cellphone that was found subsequent to a search incident to the arrest of Yan Juan Hu TAITANO See ATTACHMENT A, which is incorporated fully herein.

located in the --- District of the Northern Mariana Islands, there is now concealed *(identify the person or describe the property to be seized)*:

Evidence of violations of PConspiracy to Transport Illegal Aliens, in violation of 8 U.S.C. §§ 1324 (a)(1)(A)(ii) and (v)(I). See ATTACHMENT B, which is incorporated fully herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
8 U.S.C. §§ 1324 (a)(1)(A)(ii) and (v)(I).	Conspiracy to Transport Illegal Aliens

The application is based on these facts:

See attached Affidavit in Support of a Search Warrant, which is incorporated fully herein.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jay O. Charley, HSI Task Force Officer
Printed name and title

Sworn to before me and signed in my presence.

Date: 2/07/2024

Judge's signature

City and state: Saipan, CNMI

Ramona V. Manglona, Chief Judge
Printed name and title

AFFIDAVIT FOR SEARCH WARRANT

I, Jay O. Charley, being first duly sworn, depose and states:

Background of Affiant

1. I am a Task Force Officer with the United States Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI'). I am currently employed as a Detective for the Commonwealth of the Northern Mariana Islands ("CNMI") and I've held that position for seven (7) years. In that capacity, I serve as a TFO assigned to HSI, a position I have held for one (1) year. My training includes completion of the ICE Task Force Officer training program. I have received classroom and on the job training in the areas of general law enforcement, customs law, criminal investigative techniques, interviews and interrogations, and criminal law including arrest, search, and seizure.

2. My federal and local criminal investigative experience has involved the use of physical surveillance of individuals or premises, review and inspection of official documents and other records, and other investigative techniques. I have controlled or directly participated in criminal investigations into harboring and smuggling aliens, including the knowing intent to harbor, conceal, or shield from detection immigrants who are unlawfully present in the United States. I have also controlled, directly assisted, and participated in the execution of federal and State arrest and search warrants upon persons and premises.

3. My duties as an HSI TFO include investigating criminal violations of Federal laws outlined in Titles 18, 19, and 21 of the United States Code (U.S.C.). These Titles collectively encompass a wide range of Federal statutes such as harboring aliens, smuggling, financial and commercial investigations, materially false statements made to a federal agency, immigration benefit and/or identity fraud, passport application fraud, mail fraud, narcotics and contraband

smuggling and distribution, conspiracies to defraud the United States and other violations. Investigative techniques that I have relied upon in the course of conducting my investigations include victim, witness, and suspect interviews, review of documents and records (in paper or digital format) obtained through database checks, subpoena, court order, or consent, and physical and electronic surveillance. I have also led or participated in the execution of numerous Federal and State arrest and search warrants.

4. I am familiar with the operation of human smuggling schemes in the United States, specifically between the CNMI and the territory of Guam. I know from my training and experience that human smuggling operations often facilitate the illegal transportation of aliens from theCNMI to the territory of Guam for profit using small maritime vessels. Such vessels are typically small engine recreational boats, not intended for extended passenger voyages. I know from my experience and information relayed to me that vessels have been purchased in theCNMI with the intention of illegally transporting aliens to Guam with no intention for the vessel to return to theCNMI.

5. I know from my training and experience that Guam law requires all vessels seeking entry into the territory of Guam to provide a notice of arrival from its previous port of departure, which includes, but not limited to, the vessels registration number and crew and passenger manifests. I know from my training and experience that it is unlawful for a vessel or individual to enter the territory of Guam without inspection or approval from the Guam Customs and Quarantine Agency.

6. I know from my training and experience that aliens will pay smugglers to be illegally transported between borders and territories. I know from my experience and information relayed to me that aliens attempting illegal transportation to Guam often facilitate the smuggling

operation amongst themselves. Such facilitation includes but is not limited to the recruitment of other aliens, the purchasing of vessels, the collection of payment from intended travelers, and/or the operating of the vessel. I know from my experience that aliens have paid between $3,000 to $5,000 USD cash to be voluntarily smuggled from the CNMI to Guam. I know from my experience that aliens seek to enter Guam for higher wages compared to the CNMI. I know from my experience that aliens often enter the CNMI with the intention to overstay their legal immigration status and to work without lawful authorization.

7. I know from my training and experience that smugglers often approach the territory of Guam at secluded or uninhabited beaches, other than a designated port of entry, to offload aliens from vessels. The aliens will then make entry from the waters to the shores of the territory of Guam, in violation of Guam law.

8. Based on my training, experience, and discussions with other law enforcement officials, I am aware that it is generally common practice for persons involved in such schemes to generate and keep records pertaining to clients, payments, banking, and financial transactions. These records generally include (but are not limited to) travel records, payments made and received, checks, and correspondence using electronic mail (e-mail), social media applications, and short messaging service (SMS) texts. I know that these records are commonly generated or maintained in electronic format, using various types of electronic devices including personal desktop computers, laptop computers, personal digital assistants, tablet devices, smartphones, external hard disk drives, memory sticks, and compact discs or DVDs. I am also aware that these records are also kept in paper formats. Furthermore, these records can be transmitted via the internet using electronic devices such as personal desktop computers, laptop computers, personal digital assistants, tablet devices, and smartphones, provided the device is connected to the internet.

9. I base the information in this Affidavit on my personal knowledge and on information that I have learned, either directly or indirectly, from witnesses, records, and other law enforcement officers and agents. Additionally, unless otherwise indicated, conversations discussed herein are described in substance and part rather than verbatim. Likewise, I have not included each and every fact that my investigation has revealed, but rather, have included only those facts necessary to show probable cause.

Purpose of Affidavit

10. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing a search of: a SAMSUNG Galaxy smartphone that was found subsequent to a search incident to the arrest of Yan Juan Hu TAITANO, as further described in Attachment A, for the purpose of obtaining evidence described in Attachment B, specifically, evidence of communications and records, as well as other items associated with the illegal transportation of aliensfrom the CNMI to the territory of Guam, including any agreement or conspiracy to do so.

11. I have probable cause to believe that evidence of violations of Title 8 U.S.C. § 1324 is located in a SAMSUNG Galaxy AO4s smartphone capable of storing information electronically that was located on TAITANO's person during a search incident to arrest pursuant to a federal arrest warrant granted in the U.S. District of the Northern Mariana Islands, on or about January 29, 2024.

APPLICABLE LAWS

12. Title 8 U.S.C. § 1324(a)(1)(A)(ii) – Illegal Transportation or Attempted Transportation:

Any person who knowing or in reckless disregard of the fact that an alien has come to,

entered, or remains in the United States in violation of law, transports, or moves or attempts to transport or move such alien within the United States by means of transportation or otherwise, in furtherance of such violation of law;

13. Title 8 U.S.C. § 1324(a)(1)(A)(v)(I) – Conspiracy to Illegally Transport: Engaging in a conspiracy to transport, move, or attempting to transport or move, an alien within the United States, knowing or in reckless disregard of the fact that the alien came to, entered, and remained in the United States in violation of law.

Facts Establishing Probable Cause

14. On or about July 11, 2023, HSI Saipan initiated a criminal investigation after the United States Coast Guard conducted an emergency maritime rescue operation for eleven (11) individuals distressed on a small vessel off the coast of Rota, CNMI. The individuals were encountered by HSI investigators and subsequently identified as nine (9) non-citizens from the People's Republic of China ("PRC") and two U.S. citizens and residents of Saipan, CNMI. Independent DHS database checks further confirmed that none of the 9 PRC nationals had legal immigration status to either be present in the United States or to lawfully enter the U.S. Territory of Guam.

15. Interviews by HSI investigators with several of the PRC nationals relayed that beginning in or around June 2023, the group of PRC nationals were introduced to each other through mutual independent sources in Saipan, CNMI and began searching for a way to travel to Guam. The group were later introduced to TAITANO through mutual sources. Encountered PRC national, HongJiang YANG stated that TAITANO provided the phone number (670) 783-0968 as her contact information. Encountered PRC national, Kun GAO, furtherrelayed that TAITANO communicated through WeChat mobile application with him on the night of the group's departure

from Saipan. TAITANO sent a voice message to GAO through the WeChat application informing GAO and the group of PRC nationals that a second vessel will meet the group near Rota to continue the trip to Guam. All 9 encountered PRC nationals admitted to paying between approximately $4500-5000 USD to be transported from the CNMI to Guam on the distressed vessel, which was facilitated by TAITANO. Eight of the 9 PRC nationals subsequently provided HSI personnel with their phone numbers.

16. Subpoenaed phone records for TAITANO's known phone number, (670)783-0968, identified the number to be registered in the CNMI to TAITANO's daughter. The subscriber's listed address reflected TAITANO's known postal address, as independently verified in CNMI Department of Public Safety database checks conducted by HSI personnel. Subscriber information further identified the phone number to be registered to a Samsung Galaxy. Subpoenaed call records confirmed that beginning on or about June 19, 2023, encountered PRC nationals, YANG, ChangCai DONG, MeiFang WENG, XiaoHua LI, and YongBing TANG exchanged phone calls with TAITANO's known phone number. The encountered vessel's registered owner recorded one (1) phone call with TAITANO's known phone number on or about July 5, 2023.

17. On July 13, 2023, HSI personnel effectuated a federal search warrant on the encountered vessel in Rota, NMI, as granted by the U.S. District Court for the District of the NMI. Among searched property was a cellphone, later identified as belonging to encountered PRC national, WENG. WENG's cellphone further contained a screenshot image of a WeChat application conversation with a contact named "HU". The image, dated June 29, 2023, contained multiple exchanged voice messages and a message appearing to be sent from contact "HU" which read, "Deposit 100 received." This message corresponds to WENG and other encountered PRC nationals' statement that several members of the group paid TAITANO a down payment to

facilitate their intended transportation to Guam from Saipan.

18. On or about January 23, 2024, a federal Grand Jury in the U.S. District of the Northern Mariana Islands indicted TAITANO and three other U.S. citizens charged with conspiring to transport illegal aliens in violation of Title 8 U.S.C. §§ 1324(a)(1)(A)(ii) and (v)(I).

19. On or about January 29, 2024, TAITANO was arrested in Saipan, CNMI, by HSI personnel pursuant to a federal arrest warrant granted by the U.S. District Court for the District of theNorthern Mariana Islands. A search incident to arrest yielded the presence of a SAMSUNG Galaxy A04s smartphone on TAITANO's person. During a custodial interview by HSI personnel, TAITANO waived Miranda advisements and confirmed the smartphone was hers, and also the accuracy of TAITANO's known phone number, (670) 783-0968. TAITANO admitted to communicating by phone with several encountered PRC nationals, including meeting on multiple occasions and collecting money for the facilitation of the PRC nationals' transportation from Saipan to Guam on the encountered vessel.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

20. As described above and in Attachment B, this application seeks permission to search for records that were located on TAITANO's SAMSUNG Galaxy AO4s smartphone, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

21. *Probable cause*. I submit that if a computer or storage medium is found on the electronic devices, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

Electronically stored information that is not within the scope of the warrant will be sealed and will not be accessed or reviewed except upon a further warrant or other court order.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium found on the electronic devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United

States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The

existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

23. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be

impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. Information or evidence that is beyond the scope of the warrant will not be examined except as is necessary to determine whether or not it is within the scope of the warrant and will remain sealed until further warrant or order of the Court.

Conclusion

25. Based on the facts as set forth in this affidavit, I believe there is probable cause for a search warrant authorizing the search of the locations described in Attachment A, to seek the documents, records, and other items described in Attachment B, under violations of 8 U.S.C. §§ 1324 (a)(1)(A)(ii) and (v)(I).

26. I have shown this affidavit and the accompanying search warrant application to Assistant United States Attorney Eric O'Malley and was informed that they are in proper form.

FURTHER AFFIANT SAYETH NAUGHT

Jay O. Charley
Task Force Officer
Homeland Security Investigations

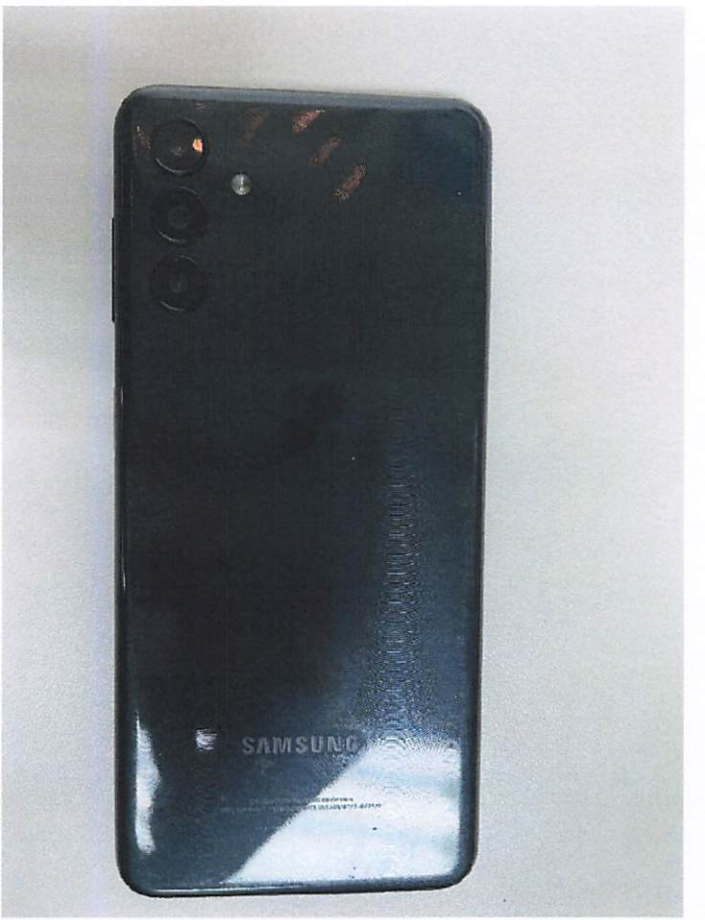
SUBSCRIBED AND SWORN TO before me on this 7th day of February 2024.

RAMONA V. MANGLONA
Chief Judge
District of the Northern Mariana Islands

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

A Samsung Galaxy A04S smartphone found on Yan Juan Hu TAITANO's person during a search incident to arrest on or about January 29, 2024, that is currently in the custody and control of Homeland Security Investigations in Saipan, Northern Mariana Islands. Pictures of the Samsung Galaxy AO4s smartphone are below:



ATTACHMENT B

ITEMS TO BE SEARCHED AND SEIZED

1. Digitally stored information and data located on the device described in Attachment A (the "DEVICE") that was used as a means to commit the violations of 8 U.S.C. §§ 1324 (a)(1)(A)(ii) and (v)(I), specifically the movement and transportation of illegal aliens from the Commonwealth of the Northern Mariana Islands to the territory of Guam.

2. Evidence of who used, owned, or controlled the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

3. Evidence indicating how and when the DEVICE was accessed or used to determine the chronological context of access, use, and events relating to crime under investigation and to the DEVICE user.

4. Evidence indicating the DEVICE user's state of mind as it relates to the crime under investigation.

5. Passwords, encryption keys, and other access devices that may be necessary to access the DEVICE.

6. Records of or information about the DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.